February 1, 2022

Challenge yourself with our Love Security quiz!

This past week's stories:

- Stolen Canadian payment card info as cheap as fancy lattes
- Why traditional insurers are struggling with cyber risk aggregation
- Gang still posting data allegedly stolen from Saskatoon airport authority
- A Canadian-themed dark market will be back, predicts expert

Security news this week: a DDoS attack wiped out Andorra's internet

More security flaws found in Apple's OS technologies

Your graphics card fingerprint can be used to track your activities across the web

China's Olympic apps may have security flaw

Phishing simulation study shows why these attacks remain pervasive

Log4j exploitations have slowed, but attack vectors remain

Experts urge firms to patch trivial-to-exploit flaw in Linux PolicyKit

Shipment-delivery scams become the favored way to spread malware

Microsoft mitigated record-breaking 3.47 Tbps DDoS attack on Azure customers

VPNLab.net shuttered in latest spate of global takedowns

Stolen Canadian payment card info as cheap as fancy lattes

A new report from NordVPN found that stolen Canadian payment card information costs, on average, just C$6.50 on black markets, cheaper than some fancy coffees.

That's half the average global cost of stolen credit card information: C$12.

https://www.itworldcanada.com/article/stolen-canadian-payment-card-info-as-cheap-as-fancy-lattes/471522

Click above link to read more.

Back to top

Why traditional insurers are struggling with cyber risk aggregation

Concerns are growing about the aggregation of cyber risks after several high-profile events in 2021 such as the SolarWinds breach, the Kaseya ransomware attack, and the Microsoft Exchange Server zero-day vulnerabilities.

Some risk aggregation events revolve around conventional metrics like industry type. For example, when the Colonial Pipeline - the largest fuel pipeline in the US - was forced to temporarily shut down its operations after falling victim to a ransomware attack, insurers knew there would be subsequent business interruption at other businesses that were dependent on the pipeline.

https://www.insurancebusinessmag.com/ca/news/cyber/why-traditional-insurers-are-struggling-with-cyber-risk-aggregation-323270.aspx

Click above link to read more.

Back to top

Gang still posting data allegedly stolen from Saskatoon airport authority

A threat actor who attacked Saskatoon's John Diefenbaker International Airport in December continues to post stolen data on its dark website in an apparent pressure tactic.

A cybersecurity industry source told *ITWorldCanada* on Friday that the Snatch gang has posted several more files today in what it calls a proof pack. The goal appears to be to embarrass the Saskatoon Airport Authority (SAA) for not paying a ransom.

It isn't clear if the gang encrypted SAA data in addition to copying files.

https://www.itworldcanada.com/article/gang-still-posting-data-allegedly-stolen-from-saskatoon-airport-authority/471756

Click above link to read more.

Back to top

A Canadian-themed dark market will be back, predicts expert

Last week's revelation that Canada's telecom regulator had pushed the dark web marketplace called Canadian HeadQuarters offline may have temporarily hurt those selling stolen credentials and malware. But a Canadian-based cybersecurity firm predicts another will take its place.

"Like Silk Road and more recently the White House marketplace takedown, it's probable that another Canadian-specific marketplace for illicit goods will likely re-appear," Ryan Westman, manager of threat intelligence team at eSentire, said in an interview.

https://www.itworldcanada.com/article/a-canadian-themed-dark-market-will-be-back-predicts-expert/471999

Click above link to read more.

Back to top

Security news this week: A DDoS attack wiped out Andorra's internet

This week hacktivism entered a new phase, as a group known as Cyber Partisans used ransomware to disrupt trains in Belarus. The hackers demanded the release of political prisoners and a promise that Belarus Railways wouldn't transport Russian troops amid mounting tensions in Ukraine. While nation state actors have deployed fake ransomware for political ends before, this appears to be the first large-scale, politically motivated use of an attack method typically reserved for cybercrime.

https://www.wired.com/story/andorra-ddos-minecraft-nso-group-security-news/

Click above link to read more.

Back to top

More security flaws found in Apple's OS technologies

Apple's software updates this week for multiple vulnerabilities in its macOS Monterey operating system, iOS, and iPadOS serve as the latest indication of security researchers' and threat actors' growing interest in its technologies.

The flaws included one in macOS that allows attackers to bypass a core OS security mechanism, two that were zero-days at the time they were disclosed, and several that allowed for arbitrary code execution with kernel-level privileges on vulnerable devices.

https://www.darkreading.com/vulnerabilities-threats/more-security-flaws-found-in-apple-s-OS-technologies

Click above link to read more.

Back to top

Your graphics card fingerprint can be used to track your activities across the web

Researchers have demonstrated a new type of fingerprinting technique that exploits a machine's graphics processing unit (GPU) as a means to track users across the web persistently.

Dubbed DrawnApart, the method "identifies a device from the unique properties of its GPU stack," researchers from Australia, France, and Israel said in a new paper," adding " variations in speed among the multiple execution units that comprise a GPU can serve as a reliable and robust device signature, which can be collected using unprivileged JavaScript."

https://thehackernews.com/2022/01/your-graphics-card-fingerprint-can-be.html

Click above link to read more.

Back to top

China’s Olympic apps may have security flaw

Security experts are warning of security flaws in a smartphone app that is mandatory for participants in the Beijing Winter Olympics.

Athletes, officials and reporters are required to use the app to keep track of their health conditions as part of coronavirus prevention measures.

But researchers at the University of Toronto say it has a vulnerability that allows third parties to extract data. They also say it is unclear how Chinese authorities plan to use the data collected by the app.

https://www3.nhk.or.jp/nhkworld/en/news/20220130_15/

Click above link to read more.

Back to top

Phishing simulation study shows why these attacks remain pervasive

Email purportedly from human resources convinced more than one-fifth of recipients to click, the majority of whom did so within an hour of receiving the fraudulent message.

A simulated phishing attack against more than 82,000 workers found that emails with a personal impact resulted in more clicks and that technical teams — such as IT workers and DevOps teams — clicked just as often and reported suspected phishing attacks less often compared with nontechnical teams

https://www.darkreading.com/threat-intelligence/simulation-shows-why-phishing-attacks-continue-to-dominate

Click above link to read more.

Back to top

Log4j exploitations have slowed, but attack vectors remain

Attackers made more than 30,000 attempts to scan and leverage exploits found in the critical Log4Shell vulnerability in January, according to security firm Kaspersky. Log4Shell, a flaw found in the Apache Software Foundation Log4j library logging tool, was first disclosed to the public in December and continues to be a challenge.

Although Kaspersky researchers say attackers are still seeking ways to facilitate the remote code execution vulnerability, the 30,562 blocked attempts mark a decline in numbers from when the flaw was originally disclosed. But cybercrime groups, such as Prophet Spider and freshly emerging ransomware gang Night Sky, have attempted to exploit the flaw.

https://www.bankinfosecurity.com/log4j-exploitations-have-slowed-but-attack-vectors-remain-a-18405

Click above link to read more.

Back to top

Experts urge firms to patch trivial-to-exploit flaw in Linux PolicyKit

The memory corruption vulnerability in a policy component installed by default on most Linux distributions allows any user to become root. Researchers have already reproduced the exploit.

A local privilege escalation of (LPE) vulnerability in the software used to handle authorizations — and installed by default — on most major distributions of Linux is trivial to exploit, with one researcher already re-creating the attack just from a detailed description of the flaw.

https://www.darkreading.com/vulnerability-management/experts-urge-firms-to-patch-trivial-to-exploit-flaw-in-linux-policykit

Click above link to read more.

Back to top

Shipment-delivery scams become the favored way to spread malware

Threat actors are increasingly using scams that spoof package couriers like DHL or the U.S. Postal Service in authentic-looking phishing emails that attempt to dupe victims into downloading credential-stealing or other malicious payloads, researchers have found.

Researchers from Avanan, a Check Point company, and Cofense have discovered recent phishing campaigns that include malicious links or attachments aimed at infecting devices with Trickbot and other dangerous malware, they reported separately on Thursday.

https://threatpost.com/shipment-delivery-scams-a-fav-way-to-spread-malware/178050/

Click above link to read more.

Back to top

Microsoft mitigated record-breaking 3.47 Tbps DDoS attack on Azure customers

Microsoft this week revealed that it had fended off a record number of distributed denial-of-service (DDoS) attacks aimed at its customers in 2021, three of which surpassed 2.4 terabit per second (Tbps).

One of the DDoS attacks took place in November, targeting an unnamed Azure customer in Asia and lasted a total of 15 minutes. It hit a peak throughput of 3.47 Tbps and a packet rate of 340 million packets per second (pps), making it the largest attack ever reported in history.

https://thehackernews.com/2022/01/microsoft-mitigated-record-breaking-347.html

Click above link to read more.

Back to top

VPNLab.net shuttered in latest spate of global takedowns

The European Union's law enforcement agency, Europol, worked with investigators in 10 nations, including the United States and Canada, to take down a virtual private network (VPN) service allegedly used by cybercriminals to hide the origin of their intrusion attempts, the group said on Jan. 20.

Law enforcement agencies from a group of 10 nations — Germany, the Netherlands, Canada, the Czech Republic, France, Hungary, Latvia, Ukraine, the United States, and the United Kingdom — worked with Europol to seize or disrupt 15 servers hosting the VPNLab.net VPN service. Starting in 2008, the service had offered encrypted communications to cybercriminals for as little as $60 a year, preventing law enforcement from tracking the source of attacks, Europol officials said in a statement. By analyzing the servers, authorities found that attacks were in progress against more than 100 businesses.

https://www.darkreading.com/attacks-breaches/vpnlab-shuttered-in-latest-spate-of-global-takedowns

Click above link to read more.

Back to top